Amendment #2
RFP NIH-NIAMS-BAA-05-02
PILOT AND FEASIBILITY TRIALS FOR OSTEOPOROSIS

Amendment to Solicitation No.:	NIH-NIAMS-05-02
Amendment No.:	2
Amendment Date:	March 10, 2005
RFP Issue Date:	January 14, 2005
Issued By:	Chief Contracting Officer Contracts Management Branch National Institute of Arthritis and Musculoskeletal and Skin Diseases, National Institutes of Health One Democracy Plaza, Suite 800, MSC 4872 6701 Democracy Boulevard Bethesda, MD 20892-4872
Point of Contact:	Dean Guidi
Name and Address of Contractor:	N/A

The above numbered solicitation is amended as set forth below.

The hour and the date specified for receipt of offers IS NOT EXTENDED.

Offerors must acknowledge receipt of the amendment prior to the hour and the date specified in the solicitation or as amended, by one of the following methods:

1. By acknowledging receipt of this amendment on each copy of the offer submitted; or
2. By separate letter, telegram, or Electronic Mail to Mr. Dean Guidi (guidid@mail.nih.gov) which includes a reference to the solicitation and amendment numbers.
3. By requesting a copy of the Standard Form 30 for this amendment and completing the information requested in items 8 and 15, and returning 1 copy of the amendment; (a hard copy of this amendment, including the Standard Form 30, may be requested from Mr. Dean Guidi (guidid@mail.nih.gov)).

FAILURE OF YOUR ACKNOWLEDGMENT TO BE RECEIVED AT THE PLACE DESIGNATED FOR THE RECEIPT OF OFFERS PRIOR TO THE HOUR AND DATE SPECIFIED MAY RESULT IN REJECTION OF YOUR OFFER.

RFP NIH-NIAMS-BAA-05-02 is hereby amended as follows:

SECTION IV, REPRESENTATIONS AND INSTRUCTIONS, is hereby modified as follows:

SECTION L.2, INSTRUCTIONS TO OFFERORS, paragraph b, Technical Proposal Instructions, is amended by adding the following paragraph regarding Information Technology Systems Security:

Information Technology Systems Security is applicable to this solicitation and the following information is provided to supplement this item to assist in proposal preparation.

(a) **Sensitivity and Security Level Designations.**

The Statement of Work (SOW) requires the successful offeror to develop or access a Federal Automated Information System (AIS). Based upon the security guidelines contained in the *Department of Health and*

Human Services (DHHS) Automated Information Systems Security Program (AISSP) Handbook, the Government has determined that the following apply:

(1) Category of Safeguarded Information

The safeguarded agency information that the successful offeror will develop or access is categorized as:

[ ] Non Sensitive Information
[X] Sensitive Information
[ ] Classified Information:
[ ] Confidential **[ ]** Secret **[ ]** Top Secret **[ ]** Special Access

(2) Security Level Designations

The information that the successful offeror will develop or access is designated as follows:

Level 2 applies to the sensitivity of the data.
Level 2 applies to the operational criticality of the data.
The overall Security Level designation for this requirement is
Level 2

(3) Position Sensitivity Designations

Prior to award, the Government will determine the position sensitivity designation for each contractor employee that the successful offeror proposes to work under the contract. For proposal preparation purposes, the following designations apply:

[ ] Level 6C: Sensitive - High Risk (Requires Suitability Determination with a BI).
Contractor employees assigned to a Level 6C position are subject to a Background Investigation (BI).

[X] Level 5C: Sensitive - Moderate Risk (Requires Suitability Determination with NACIC).
Contractor employees assigned to a Level 5C position with no previous investigation and approval shall undergo a National Agency Check and Inquiry Investigation plus a Credit Check (NACIC), or possibly a Limited Background Investigation (LBI).

[ ] Level 4C: Classified (Requires Special Access Clearance with an SSBI).
Contractor employees assigned to a Level 4C position are subject to a Single Scope Background Investigation (SSBI).

[ ] Level 3C: Classified (Requires Top Secret Clearance with an SSBI).
Contractor employees assigned to a Level 3C position are subject to a Single Scope Background Investigation (SSBI).

[ ] Level 2C: Classified (Requires Confidential or Secret Clearance with an LBI).
Contractor employees assigned to a Level 2C position shall undergo a Limited Background Investigation (LBI).

[ ] Level 1C: Non Sensitive (Requires Suitability Determination with an NACI).
Contractor employees assigned to a Level 1C position are subject to a National Agency Check and Inquiry Investigation (NACI).

Upon award, the contractor will be required to submit a roster of all IT staff working under the contract. The Government will determine the appropriate level of suitability investigation required for each staff member.

Contractor employees who have met investigative requirements within the past five years may only require an updated OR upgraded investigation.

(b) **Information Technology (IT) System Security Program**

The offeror's proposal must:

(1) Include a detailed System Security Plan (SSP) of its present and proposed IT systems security program commensurate with the size and complexity of the requirements of the Statement of Work. Template for a full System Security Plan are available at:

(i) SSP Template (detailed)
http://irm.cit.nih.gov/security/secplantemp.doc

(ii) Security Plan Outline (outline only)
http://irm.cit.nih.gov/nihsecurity/Security_Plan_Outline.doc

(2) Demonstrate that it complies with the AISSP security requirements, the Computer Security Act of 1987; Office of Management and Budget (OMB) Circular A-130, Appendix III, "Security of Federal Automated Information Systems;" and the DHHS AISSP Handbook.

At a minimum, the offeror's proposed information technology systems security program must address the minimum requirements of a s**ecurity Level _2_** identified in the DHHS AISSP Handbook, Exhibit III-A, Matrix of Minimum Security Safeguards.

Examples of the minimum areas to be addressed include, but are not limited to administrative, technical, and physical security as follows:

(i) Security Awareness Training
(ii) Access Control
-Network (ex: firewall)
-System (ex: network OS, tcp wrappers, SSH)
-Application (ex: S-LDAP, SSL)
-Remote Access (ex: VPN)
-Monitoring and support (ex: IDS, pager, NOC)
(iii) Protection against data loss
-OS security (ex: patch management, configuration)
-Application security (ex: patch management)
-Database security
-Back-up and recovery
-Fault tolerance, high availability
(iv) Malicious Code Protection (ex: Antivirus, filtering of e-mail attachments, etc)
(v) Physical Security
-Access control (ex: locks, guards)
-Power condioning and/or UPS
-Air conditioning
-Fire protection

(3) Include an acknowledgment of its understanding of the security requirements.

(4) Provide similar information for any proposed subcontractor developing or accessing an AIS.

(c) **Required Training for IT Systems Security**

DHHS policy requires that contractors receive security training commensurate with their responsibilities for performing work under the terms and conditions of their contractual agreements.

The successful offeror will be responsible for assuring that each contractor employee has completed the following NIH Computer Security Awareness Training course prior to performing any contract work: http://irtsectraining.nih.gov/. The contractor will be required to maintain a listing of all individuals who have completed this training and submit this listing to the Government.

Additional security training requirements commensurate with the position may be required as defined in OMB Circular A-130 or NIST Special Publication 800-16, "Information Technology Security Training Requirements." These documents provide information about IT security training that may be useful to potential offerors.

(d) **References**

The following documents are electronically accessible:

(1) OMB Circular A-130, Appendix III: http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html
(2) DHHS AISSP Handbook: http://irm.cit.nih.gov/policy/aissp.html
(3) DHHS Personnel Security/Suitability Handbook: http://www.hhs.gov/ohr/manual/pssh.pdf
(4) NIH Applications/Systems Security Template http://irm.cit.nih.gov/security/secplantemp.doc
(5) NIH Security Plan Outline: http://irm.cit.nih.gov/nihsecurity/Security_Plan_Outline.doc
(6) NIST Special Publication 800-16, "Information Technology Security Training Requirements:" http://csrc.nist.gov/publications/nistpubs/800-16/800-16.pdf Appendix A-D: http://csrc.nist.gov/publications/nistpubs/800-16/AppendixA.pdf
(7) NIH CIT-Policies, Guidelines and Regulations:
Table 1 - Categories of Safeguarded Agency Information: http://irm.cit.nih.gov/security/table1.htm
Table 2 - Security Level Designations for Agency Information: http://irm.cit.nih.gov/security/table2.htm
Table 3 - Positions Sensitivity Designations for Individuals Accessing Agency Information: http://irm.cit.nih.gov/security/table3.htm
(8) NCI Information Technology Security Policies, Forms and Procedures for Contracts: http://ais.nci.nih.gov/